

AMENDMENTS TO THE SPECIFICATION:

Please amend paragraphs 27 and 28 of the Specification as follows.

There are two main cryptographic methods that may be suitable for use with system 100. The traditional method uses a secret key, such as the Data Encryption Standard (DES). In DES, both sender and receiver use the same key to encrypt and decrypt. This is the fastest method, but transmitting the secret key to the recipient in the first place is not secure. The second method is public-key cryptography, such as the Rivest-Shamir-Adleman (RSA) highly-secure cryptography method by RSA Data Security, Inc., Redwood City, CA, (~~www.rsa.com~~). RSA uses a two-part concept with both a private and a public key. The private key is kept by the owner; the public key is published. Each recipient has a private key that is kept secret and a public key that is published for everyone. The sender looks up the recipient's public key and uses it to encrypt the message. The recipient uses the private key to decrypt the message. Owners never have a need to transmit their private keys to anyone in order to have their messages decrypted, thus the private keys are not in transit and are not vulnerable.

Public key cryptography software marketed under the name Pretty Good Privacy (PGP) from Pretty Good Privacy, Inc., (PGP) of San Mateo, CA, (~~www.pgp.com~~) may be utilized in this embodiment. PGP was developed by Phil Zimmermann, founder of the company, and it is based on the RSA cryptographic method. A version for personal, non-business use is available on various Internet hosts. While PGP may be used to encrypt data transmitted over network 110, those skilled in the art will appreciate that many other types of encryption algorithms, methods and schemes may be employed.